Abstract Algebra in Theoretical Computer Science

Final Exam

Lecturer: Gil Cohen

Problem 1

Let G be a finite abelian group. Let $m = \max_{g \in G} o(g)$ be the maximal order of elements in G. Prove that $o(g) \mid m$ for every $g \in G$.

Problem 2

Let R be a commutative ring. Prove that if $R[x]$ is a PID then R is a field. You may use, without a proof, the (easy) fact: $R[x]/\langle x \rangle \cong R$.

Problem 3

Let R be a commutative ring and I an ideal in R. Recall that the radical of I is defined by $\sqrt{I} = \{r \in R \mid r^n \in I \text{ for some } n \in \mathbb{N}\}$. Prove that $\sqrt{I}$ is an ideal.

Problem 4

Let $R = \mathbb{Z}[i]/\langle i - 1 \rangle$. What is the strongest structure you can guarantee R has, namely, is it a ring that is not a domain or rather it is a domain / PID / field? What is the size of R? No proof is required.

Problem 5

Let K/F be a field extension. Let $a, b \in K$ be algebraic elements over F. Prove that $a + b$ is algebraic over F.

Problem 6

Consider the irreducible polynomial $x^2 + x + 1 \in \mathbb{F}_2[x]$ and let $\mathbb{F} = \mathbb{F}_2[x]/\langle x^2 + x + 1 \rangle$ be the field of 4 elements. List *all* monic degree 2, irreducible polynomials in $\mathbb{F}[y]$. No proof / calculations are required - just the list.

Problem 7

1. List all subfields of the field of 1024 elements. Prove your answer.
2. How many degree 10 irreducible polynomials over $\mathbb{F}_2$ are there? Prove your answer.

Problem 8

Let q be a prime power. A set $N \subseteq \mathbb{F}_q^3$ is said to be *line-friendly* if for at least half the elements $x \in \mathbb{F}_q^3$ there exists $y = y(x) \in \mathbb{F}_q^3 \setminus \{0\}$ such that

$$|N \cap \{x + ty \mid t \in \mathbb{F}_q\}| \geq q/2.$$

Give the best lower bound you can on the size of any line-friendly set. I care only about the asymptotic behavior with respect to q and there is no need to optimize the multiplicative constant.

Problem 9

Let q be a prime power and $n \geq 1$ an integer. A set $S \subseteq \mathbb{F}_q^n$ is *pairwise linearly independent* if every distinct elements $a, b \in S$ are linearly independent over $\mathbb{F}_q$.

Assume n is even, $n = 2m$. In this question we will construct a large pairwise linearly independent set in $\mathbb{F}_q^n$. As was done throughout the course, we fix an $\mathbb{F}_q$-vector space isomoprhism between $\mathbb{F}_q^m$ and $\mathbb{F}_{q^m}$. We abuse notation and for an element $v \in \mathbb{F}_{q^m}$ denote by v the corresponding vector in $\mathbb{F}_q^m$.

We define the set $S \subseteq \mathbb{F}_q^n$ as follows. Every element in S is indexed by a nonzero field element $a \in \mathbb{F}_{q^m}$. The corresponding element in S is defined by (a, a^2). That is, the first m coordinates are a (thought of as a vector in $\mathbb{F}_q^m$) and the last are a^2.

1. Prove that S is pairwise linearly independent. What is its size? (I would like to remark that there are larger pairwise linearly independent sets but let's focus on this one).

2. An enthusiastic student who solved the first item of this question suggested that the choice (a, a^2) is essentially arbitrary and that, say, (a, a^3) would do the job just as well. Is this correct for all q, n?

3. Give a sufficient and necessary condition on q, n so that the choice (a, a^4) works. The condition should be phrased without any reference to groups, rings, or fields - just an elementary relation on the numbers q, n (e.g, $q^2 \equiv n^3 \mod 5$). Prove your answer.

Problem 10

For every integer n and $0 < \varepsilon < 1$ construct an ε-biased set $S \subseteq \{0,1\}^n$ of size

$$|S| = O((n/\varepsilon^3) \cdot \log^2(n/\varepsilon)).$$

Analyze your construction.

Hint: Let ℓ be a parameter and $S_0 \subseteq \{0,1\}^\ell$ be a small-bias set obtained by the powering construction. The elements of your set S should be indexed by a pair $(x, y) \in \mathbb{F}_{2^\ell} \times S_0$.